We claim:

1. A cryptographic device, comprising:

means for performing one or more cryptographic operations; and

a data storage device for storing access permission data representing an availability of one or more cryptographic characteristics in accordance with which one or more of the cryptographic operations are performed, wherein once a value or values of the access permission data are stored in the data storage device, the value or values of the access permission data cannot be changed.

2. A cryptographic device as in Claim 1, wherein the data storage device is a programmable read-only memory.

3. A cryptographic device as in Claim 1, wherein the cryptographic characteristics include one or more of the following: availability of direct access to one or more mathematical primitive operations, availability of public key encryption, permissible maximum length of public key, permissible maximum length of DES key, and availability of DES key encryption.

4. A computer readable storage medium on which access permission data is stored in accordance with a predefined data structure, the access permission data representing an availability of one or more cryptographic characteristics in accordance with which one or more of cryptographic operations are performed by a cryptographic device, wherein once a value or values of the access permission data are stored on the storage medium, the value or values of the access permission data cannot be changed.

5. A computer readable storage medium as in Claim 4,

wherein the cryptographic characteristics include one or more of the following: availability of direct access to one or more mathematical primitive operations, availability of public key encryption, permissible maximum length of public key, permissible maximum length of DES key, and availability of DES key encryption.

6. A cryptographic device, comprising:

a processor for executing instructions and/or accessing data to perform one or more cryptographic operations that each necessitate the performance of one or more sub-operations; and

one or more data storage devices for storing a first set of instructions and/or data used to perform one or more sub-operations of a cryptographic operation, and a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform the one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-operations are performed; and

means for allowing access to the first set of instructions and/or data from a device external to the cryptographic device.

7. A cryptographic device as in Claim 6, wherein the one or more sub-operations comprise one or more mathematical primitive operations.

8. A cryptographic device as in Claim 7, wherein the mathematical primitive operations include one or more of the following: a mod reduce operation, an add operation, a subtract operation, a multiply operation, a divide operation,

an exponentiate operation, an inverse modulo operation, an XOR operation, a DES operation and an random number generator operation.

9. A cryptographic device as in Claim 6, wherein the cryptographic operations include one or more of the following: RSA encrypt, RSA decrypt, DSA sign, DSA verify, Diffie-Hellman and elliptic curve.

10. A cryptographic device as in Claim 6, wherein the first set of instructions and/or data used to perform one or more sub-operations are stored in a read-only memory device.

11. A cryptographic device as in Claim 10, wherein at least some of the second set of instructions and/or data used to perform the one or more cryptographic operations are stored in an erasable programmable read-only memory device.

12. A cryptographic device as in Claim 11, wherein at least some of the second set of instructions and/or data used to perform the one or more cryptographic operations are stored in a read-only memory device.

13. A cryptographic device as in Claim 6, wherein at least some of the second set of instructions and/or data used to perform the one or more cryptographic operations are stored in an erasable programmable read-only memory device.

14. A computer readable storage medium encoded with one or more computer programs for enabling performance of cryptographic operations, comprising:

a first set of instructions and/or data used to perform one or more sub-primitive operations; and

a second set of instructions and/or data, distinct from the first set of instructions and/or data, used to perform one or more cryptographic operations, wherein the second set of instructions and/or data includes one or more instructions that cause performance of instructions and/or access of data from the first set of instructions and/or data so that one or more of the sub-sub-operations are performed; and

a third set of instructions and/or data for allowing and mediating access to the first set of instructions and/or data from a device external to a device of which the computer readable storage medium is part.

15. A cryptographic device as in Claim 14, wherein the one or more sub-operations comprise one or more mathematical primitive operations.

16. A computer readable storage medium as in Claim 15, wherein the mathematical primitive operations include one or more of the following: a mod reduce operation, an add operation, a subtract operation, a multiply operation, a divide operation, an exponentiate operation, an inverse modulo operation, an XOR operation, a DES operation and an random number generator operation.

17. A computer readable storage medium as in Claim 13, wherein the cryptographic operations include one or more of the following: RSA encrypt, RSA decrypt, DSA sign, DSA verify, Diffie-Hellman and elliptic curve.